REMARKS

Reconsideration and allowance of the subject application in view of the foregoing amendments and the following remarks is respectfully requested. Entry of this Response Under Rule 116 is merited as it raises no new issues and requires no further search.

Claims 1-19 are pending.

The following remarks are provided in response to the Examiner's Response to Arguments at page 2, section 2 of the Final Official Action mailed on August 26, 2005. The Examiner asserts that the adding, deleting, or changing of any files as described by Kim et al. ("The Design and Implementation of Tripwire: A File System Integrity Checker") at page 27, paragraph 4, is analogous to "reading events representing various types of system calls" as claimed in the present subject matter. The Examiner is incorrect as Kim merely describes the provision of a mechanism to determine file changes, specifically the addition, deletion, and changing of a file, without reading events representing system calls. A rejection based on 35 U.S.C. 102 requires every element of the claim to be included in the reference, either directly or inherently, and the Examiner has failed to identify every claim element in Kim. Kim scans a file system to determine whether any files have been added, deleted, or changed. As previously described in the response filed June 7, 2005, events as described in the instant specification include kernel audit records which pertain to system call invocations by a process. Files are not events. Scanning files to determine changes is not the same as reading events representing various types of system calls. There is no disclosure in Kim of reading events.

Further, the Examiner asserts that page 25, paragraph 1 of Kim describes determining whether a change was a wanted change or a result of an intruder, whereby an alert is created; however, there is no such disclosure in the cited portion of Kim. The cited portion of Kim describes that a filename is printed if any attributes are to be monitored according to a selection-mask without regard to whether a change was wanted or a result of an intruder. The Examiner is requested to specifically identify any support in the cited portion for the Examiner's assertions regarding wanted/unwanted changes versus intruder-based changes.

For one or both of the foregoing reasons, claim 1 is patentable over Kim and the rejection should be withdrawn.

Further, Applicant's arguments advanced previously in the Amendment filed June 7, 2005 apply notwithstanding the Examiner's erroneous and groundless assertion regarding equivalence of files and events. Applicant's arguments are re-presented herein for ease of reference.

A rejection based on 35 U.S.C. §102 requires every element of the claim to be included in the reference, either directly or inherently. Kim fails to anticipate the subject matter of claim 1 as Kim fails to disclose reading events representing various types of system calls. Kim is directed to a tool for monitoring a designated set of files and directories for any changes and not to reading events as in the claimed subject matter. Kim is "[u]sed with system files on a regular (e.g., daily) basis." Kim at Abstract. The Examiner's attention is directed to page 4, lines 7-10 of the present specification for a brief description of events, e.g., "'[e]vents' in this context are kernel audit records read from the IDDS subsystem." Events include kernel audit records, which pertain to system call invocations by a process. In contrast, Kim describes employing signature routines to identify changes in files without reading events as in the claimed subject matter. For at least this reason, claim 1 is patentably distinguishable from Kim and the rejection should be withdrawn.

Claims 1-19 depend, either directly or indirectly, from claim 1 and 14, include further important limitations, and are patentable over Kim for at least the reasons advanced above with respect to claim 1 and claim 14. The rejection of claims 1-19 should be withdrawn.

Claim 7 is patentable over Kim for reasons similar to those advanced above with respect to claim 1. The rejection of claim 7 should be withdrawn.

Claims 8-12 depend from claim 7, include further important limitations, and are patentable over Kim for at least the reasons advanced above with respect to claim 7. The rejection of claims 8-12 should be withdrawn.

Claim 14 is patentable over Kim for reasons similar to those advanced above with respect to claim 1 and the rejection should be withdrawn. Claims 15-19 depend, either directly or indirectly, from claim 14, include further important limitations, and are patentable over Kim for at least the reasons advanced above with respect to claim 14. The rejection of claims 15-19 should be withdrawn.

All objections and rejections having been addressed, it is respectfully submitted that the present application should be in condition for allowance and a Notice to that effect is earnestly solicited.

Early issuance of a Notice of Allowance is courteously solicited.

The Examiner is invited to telephone the undersigned, Applicant's attorney of record, to facilitate advancement of the present application.

To the extent necessary, a petition for an extension of time under 37 C.F.R. 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 07-1337 and please credit any excess fees to such deposit account.

Respectfully submitted,

LOWE HAUPTMAN & BERNER, LLP

Randy A. Noranbrock

Randy A. Noranbrock
Registration No. 42,940

USPTO Customer No. 22429
1700 Diagonal Road, Suite 300
Alexandria, VA 22314
(703) 684-1111
(703) 518-5499 Facsimile
Date: October 25, 2005
KMB/RAN/iyr